GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

April 27, 2017

Mr. Terry Rice
Vice President, IT Risk Management
Chief Information Security Officer
Merck & Company, Inc.
2000 Galloping Hill Road
Kenilworth, NJ 07033

Dear Mr. Rice:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, April 4, 2017, to testify at the hearing entitled "Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Thursday, May 11, 2017. Your responses should be mailed to Elena Brennan, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Elena.Brennan@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

cc: The Honorable Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachment

Attachment—Additional Questions for the Record

The Honorable Tim Murphy

1. I understand that HHS, apparently at the request of DHS, is establishing a Cybersecurity Communications and Integration Center specific to the health care sector, the "HCCIC." It would appear that this organization, at least on some level, replicates the role of an ISAC in other sectors.

    a. What is your understanding of this effort and how does it relate to your organization?

    b. Based on your experience, are there other sectors that have their own CCIC?

    c. Do you think this will be beneficial in addressing some of the challenges in the health care sector?

    d. Are there any potential downsides to having an "HCCIC?" If so, what are they?

2. According to the membership roster, each of your organizations is a member of the Healthcare and Public Health Sector Coordinating Council. We know the Healthcare SCC has many roles and responsibilities beyond cybersecurity, but as cybersecurity becomes more important across the industry, the SCC will arguably have a big role to play. What services, products or value does the SCC offer regarding cybersecurity?

    a. Do you get the sense that their role and contributions are understood and appreciated across the sector?

    b. Are there ways that the SCC could be more effective in assisting the sector with cybersecurity challenges?

3. My staff and I have heard from stakeholders in other industries, most notably the electricity sector, that they have broad, senior executive level engagement on their SCC, and that this engagement has significantly increased the effectiveness of the council and other aspects of their public-private partnerships, such as their ISAC. Who from your organizations participates in the Healthcare SCC?

    a. Would a similar model, with broad senior executive engagement on the SCC, work in the health care sector? Why or why not?

    b. Do you have any other thoughts on the SCC and its importance or the roles it plays in health care sector cybersecurity?

4. As the Sector Specific Agency for the healthcare sector, HHS has a big role to play in guiding and supporting industry cybersecurity efforts. Can each of you briefly tell us how HHS, as the SSA for your sector, provides cybersecurity guidance and support for your organization?

a. Who in HHS, or what office, is considered the "go-to" contact for cybersecurity issues?

5. My understanding is that that there are multiple agencies within HHS that have pieces of healthcare cybersecurity. For example, the Office of Civil Rights deals with data breaches, the Food and Drug Administration deals with medical devices, and the list goes on for other components of the agency. What parts of HHS does Philips work with when it comes to cybersecurity?

    a. Does this division of cybersecurity roles and responsibilities at HHS complicate the ability of Merck to address cybersecurity within its products and organization?

    b. Would additional coordination or clarity by HHS regarding which pieces of the agency have responsibility for cybersecurity, and when, help your organizations?

    c. Do you have any suggestions for actions that HHS could take to better coordinate or clarify its cybersecurity roles and responsibilities?

6. The public-private partnership model depends on trust and collaboration between government and private sector participants. This can prove challenging in some sectors, such as health care, where the Sector Specific Agency (SSA) is also the regulator for that sector. Some sectors – such as financial services – have overcome these challenges to develop a robust relationship with their SSA. How much does the success of a public private partnership for cybersecurity depend on the level of trust and collaboration between private sector participants and their government counterparts, especially their sector specific agency?

    a. Is this a challenge in the health care sector, where HHS is the Sector Specific Agency but also serves as the regulator?

    b. Does the fact that different parts of the health care sector are regulated by different components of HHS complicate this relationship?

    c. Based on your experience, have other industries managed to navigate a similar situation, where their Sector Specific Agency is also their regulator? Or are there challenges unique to the health care sector its relationship to HHS that further complicate this dynamic?

7. Your organization is obviously larger and more well-resourced than a rural hospital or small physician practice. We've seen in other cases like the Target breach, however, that smaller organizations can be the "infection points" for larger organizations, due to the way that business relationships and networks are set up. Recognizing that cybersecurity is a collective responsibility, how do – or can – larger organizations assist in bolstering awareness and engagement of smaller participants in the sector?

    a. Are there factors that impede collaboration within the sector?

8. During the hearing, we talked a great deal about the HHS as the SSA, and the NH-ISAC, but we didn't really touch on the Government Coordinating Council. What role does the GCC play for each of your organizations?

    a. Are there additional initiatives that you believe that the GCC could take, or roles that it could fill, that would help your organizations and the health care sector as a whole better address cybersecurity?

9. Would you support HHS making a recommendation that encourages participation in the ISAC?

    a. Do you believe that it would improve the functioning of the ISAC, and therefore cybersecurity across the sector, for HHS to make such a recommendation?

    b. Do you think there are potential consequences – real or perceived – from HHS taking this approach?

10. Recently in the cybersecurity community, there has been some confusion regarding ISACs and ISAOs. Do you think that this confusion has caused any issues with regards to cybersecurity protocol – specifically facilitating effective situational awareness and response activities, particularly when an incident occurs?

    a. What do you think should be done to address this confusion?

The Honorable Buddy Carter

1. When we think about cybersecurity and health, most people seem to understand the dangers regarding privacy of their personal health information. But, what most people don't know is that this kind of theft can have a direct impact on your health. As a pharmacist, I also know that if we don't catch medical identify fraud, it can have serious physical consequences for patients. Can you elaborate on the consequences of medical identity theft?

2. The GAO recently released a study analyzing Identity Theft Services. The report details the dangers that we have discussed here. Have you reviewed this study? How do you propose that we counter these very real threats to our health care?